UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte GERALD F. MCBREARTY, SHAWN P. MULLEN, JOHNNY MENG-HAN SHIEH, and MICHAEL W. WORTMAN

Appeal 2006-2685
Application 09/801,614
Technology Center 2100

Decided: March 26, 2007

Before JAMES D. THOMAS, MAHSHID D. SAADAT, and JEAN R. HOMERE, *Administrative Patent Judges*.

SAADAT, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30. Claims 2, 3, 6, 8, 9, 11, 12, 15, 16, 18, 19, 22, 23, 26, 28, and 29 have been canceled.

We reverse.

BACKGROUND

Appellants' invention relates to security of data files by setting up for destruction of intruded files as soon as an intrusion is suspected. For each file, a duplicate or a backup, which remains substantially inaccessible to user requests, is stored for reloading after the compromised data is destroyed (Specification 3-4). An understanding of the invention can be derived from a reading of exemplary independent claim 1, which is reproduced as follows:

1. In a data processing operation having stored data in a plurality of data files, a system for protecting said data files from unauthorized user comprising:

means for storing for each of said plurality of data files, a backup file inaccessible to user requests;

means for receiving user requests for access to data files;

means for determining whether said requests are unauthorized intrusions into said requested data files;

means responsive to an initial determination that a request is unauthorized for destroying the requested data files; and

means for reloading a backup file for each destroyed file.

The Examiner relies on the following references:

Schneck	US 5,933,498	Aug. 3, 1999
Groshon	US 6,351,811 B1	Feb. 26, 2002

Claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneck in view of Groshon.

The Examiner relies on Schneck for disclosing the claimed storage and protection of data against unauthorized intrusions and on Groshon for teaching storage of backup files for each data file wherein the backup files are inaccessible to the users (Answer 3-4). The reason for such combination is stated by the Examiner as the desire for making un-compromised copies available as needed (Answer 4). Appellants argue that Schneck fails to teach storing backup files as well as reloading a backup file for each destroyed file (Br. 5). Appellants further assert that the possibility of transmitting and using compromised and suspect data in Groshon actually teaches away from the proposed combination and would not result in substituting the stored backup files for the files that are destroyed after unauthorized intrusion is determined, as recited in the claims (Br. 5-6). Thus, the issue before this panel is whether one of ordinary skill in the art would have been motivated to properly combine Schneck and Groshon and the combination discloses all the claimed features.

OPINION

As a general proposition, in rejecting claims under 35 U.S.C. § 103, the Examiner bears the initial burden of presenting a prima facie case of obviousness. *See In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993) and *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598

(Fed. Cir. 1988). Furthermore, the conclusion that the claimed subject matter is prima facie obvious must be supported by evidence, as shown by some objective teaching in the prior art or by knowledge generally available to one of ordinary skill in the art that would have led that individual to combine the relevant teachings of the references to arrive at the claimed invention. See *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

After reviewing Groshon, we agree with Appellants that the reference teaches against modifying Schneck to destroy the requested data in case of unauthorized intrusion as Groshon provides for circumstances in which the requested data is transmitted even if it is determined to have been compromised (col. 6, ll. 26-37). Although Groshon teaches storing backup Web pages (col. 4, l. 64-col. 5, l. 3), the backup files are not used for substituting the compromised files that are destroyed. Instead, the backup is used for validation by comparing a Web page prior to its transmission with the backup copy (col. 5, ll. 3-9) or transmission in place of the page whose signature is not identical to a controlled signature (col. 6, ll. 28-32). However, if no backup is available, Groshon sends the compromised data along with a message notifying the recipient that the data is suspect (col. 6, ll. 32-37). Therefore, Groshon is concerned with the authenticity of the data, and not whether the request is authorized, for keeping or destroying the requested data. Even when the data is determined to be compromised, Groshon may transmit the backup file if a backup exists or transmit the compromised data with along with a message to indicate that the data is

suspect. As argued by Appellants (Reply Br. 3), nowhere does Groshon teach or suggest that the requested data is necessarily destroyed and a backup file is reloaded for each destroyed file if the request for data is unauthorized.

Schneck, on the other hand, controls access to protected data by identifying unauthorized access and erasing the memory before its contents may be read (col. 16, ll. 47-56). However, contrary to the Examiner's assertion (Answer 5), the tamper detection system of Schneck does not suggest storing backup files for each data file and reloading the stored backup file for each erased file.

A rejection based on section 103 must rest upon a factual basis rather than conjecture, or speculation. "Where the legal conclusion [of obviousness] is not supported by facts it cannot stand." *In re Warner*, 379 F.2d 1011, 1017, 154 USPQ 173, 178 (CCPA 1967). See also *In re Lee*, 277 F.3d 1338, 1344, 61 USPQ2d 1430, 1434 (Fed. Cir. 2002) and *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). Here, we also remain unconvinced by the Examiner's assertions (Answer 10-11) that the claimed reloading the backup files for the destroyed files would have been obvious in view of Groshon's use of backup file for a compromised data since Groshon does not teach that the compromised files are destroyed or the backup file is necessarily transmitted. As discussed above, Groshon merely suggests that a backup file may be transmitted without requiring destruction of the compromised data and reloading the backup file or the compromised data may be transmitted with an error message.

Thus, the disclosures of Schneck and Groshon fall short of teaching or suggesting that the requested data is destroyed and a backup file is reloaded for each destroyed file if the request for data is unauthorized. We also note that the other independent claims require similar determination and destruction of unauthorized requests and reloading of the backup files which are neither taught nor suggested by the proposed combination of the references. Accordingly, as the Examiner has failed to set forth a prima facie case of obviousness with respect to any of the independent claims, we cannot sustain the 35 U.S.C. § 103 rejection of claims 1, 5, 7, 10, 14, 17, 21, 25, and 27, nor of their dependent claims 4, 13, 20, 24, and 30, over Schneck and Groshon.

CONCLUSION

In view of the foregoing, the decision of the Examiner rejecting claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30 under 35 U.S.C. § 103 is reversed.

REVERSED

tdl/ce

International Business Machines Corporation
Intellectual Property Law Department
Internal Zip 4054
11400 Burnet Road
Austin, TX 78758